UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT
EASTERN DIVISION OF OHIO

In the Matter of the Search of:	)	**No.** 2:24-MJ-324
	)	
The email account, including all information and Content, associated with the Google email address israthshikdar@gmail.com and referred to as the SUBJECT ACCOUNT, that is stored at the Premises Controlled by Google, Inc.	)	**Magistrate Judge** DEAVERS
	)	
	)	**UNDER SEAL**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Amanda North (Your Affiant), a Special Agent with the Ohio Bureau of Criminal Investigation (BCI) and assigned as a Task Force Officer (TFO) for the Federal Bureau of Investigation (FBI), being duly sworn, hereby depose and state:

EDUCATION TRAINING AND EXPERIENCE

1. I am a Special Agent (SA) with BCI, since 2022, and have been in the Special Victims Unit since 2013, where I was previously a Criminal Investigator. I have been a TFO at the FBI Columbus Resident Agency since early 2023. I am primarily responsible for investigating child sexual exploitation and internet crimes, as well as hands on offenses of abuse involving juveniles and the elderly.

2. During my career as a Criminal Investigator, I have received more than one hundred hours of training in internet investigations, to include Peer to Peer software. I was assigned full-time to the Franklin County Internet Crimes Against Children Task Force (ICAC), from January of 2016 through my promotion to SA in May of 2022. I was also a TFO for Homeland Security from 2018 until the end of 2021, when I was designated to be assigned to the FBI VCAC Unit. I have participated in various investigations of child exploitation and have executed numerous search warrants, interviews and arrests that resulted in conviction. As part of my duties as a TFO, I investigate criminal violations relating to child exploitation and child

pornography violations, including the illegal production, distribution, transmission, receipt, and possession of child pornography, in violation of 18 U.S.C. §§ 2251, 2252, and 2252A.

3. As a TFO with the FBI, I am authorized to investigate violations of the laws of the United States and to execute warrants issued under the authority of the United States.

PURPOSE OF THE AFFIDAVIT

4. I make this affidavit in support of an application for a search warrant for information associated with the following email address from a Google email account israthshikdar@gmail.com that is stored at premises controlled by Google, a Google of electronic communications service and remote computing service headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043. The information to be searched is described in the following paragraphs and in **Attachment A**. This affidavit is made in support of an application for a search warrant under 18 U.S.C. 875 to require Google, Inc. to disclose to the government records and other information in its possession, including the contents of communications, pertaining to the subscriber or customer associated with the **SUBJECT ACCOUNT.**

5. The **SUBJECT ACCOUNT** to be searched is more particularly described in **Attachment A**, for the items specified in **Attachment B**, which items constitute instrumentalities, fruits, and evidence of violations of 18 U.S.C. 875– extortion via interstate communications. I am requesting authority to search the **SUBJECT ACCOUNT**, wherein the items specified in **Attachment B** may be found, and to seize all items listed in **Attachment B** as instrumentalities, fruits, and evidence of crime.

6. The facts set forth below are based upon my knowledge, experience, observations, and investigation, as well as the knowledge, experience, investigative reports, and information provided to me by other law enforcement agents. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every known fact to me relating to the investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. 875(d) – extortion via interstate communications are presently located in the **SUBJECT ACCOUNT.** I have not omitted any facts that would negate probable cause.

APPLICABLE STATUTES AND DEFINITIONS

7. Title 18, United States Code, Section 875, makes it a federal crime for any person to, with the intent to extort from another person, firm, association, or corporation, any money or thing of value, to transmit in interstate or foreign commerce any communication containing any threat to injure the property or reputation of the addressee of another.

8. The term "computer"[2] is defined in Title 18 U.S.C. § 1030(e)(1) and 2256(6) as an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.

9. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

10. "Cellular telephone" or "cell phone" means a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books"; sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving videos; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may include geographic information indicating where the cell phone was at particular times.

11. "Internet Service Providers" (ISPs), used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.

12. "Internet Protocol address" (IP address), as used herein, is a code made up of numbers separated by dots that identifies particular computer on the Internet. Every computer requires an IP address to connect to the Internet. IP addresses can be dynamic, meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet.

BACKGROUND INFORMATION REGARDING GOOGLE, GMAIL, AND TECHNOLOGY

13. Google, LLC provides its subscribers internet-based accounts that allow them to send, receive, and store e-mails online. Google accounts are typically identified by a single username, which serves as the subscriber's default e-mail address, but which can also function as a subscriber's username for other Google services, such as instant messages and remote photo or file storage.

14. Based on my training and experience, I know that Google allows subscribers to obtain accounts by registering on Google's website. During the registration process, Google asks subscribers to create a username and password, and to provide basic personal information such as a name, an alternate e-mail address for backup purposes, a phone number, and, in some cases, a means of payment. Google typically does not verify subscriber names. However, Google does verify the e-mail address or phone number provided.

15. Once a subscriber has registered an account, Google provides e-mail services that typically include folders such as an "inbox" and a "sent mail" folder, as well as electronic address books or contact lists, and all of those folders are linked to the subscriber's username. Google subscribers can also use that same username or account in connection with other services provided by Google.

16. Notably, Google, LLC also provides "cloud" storage services. Account holder/users can utilize this service, which is called "Google Drive," to store pictures, videos,

and other electronic files remotely and without taking up memory space on their personal computer, smart phone, and physical storage media.

17. In general, user-generated content (such as e-mail) that is written using, stored on, sent from, or sent to a Google account can be permanently stored in connection with that account, unless the subscriber deletes the material. For example, if the subscriber does not delete an e-mail, the e-mail can remain on Google servers indefinitely. Even if the subscriber deletes the e-mail, it may continue to exist on Google's servers for a certain period of time.

18. These services may include electronic communication services such as Google Voice (voice calls, voicemail, and SMS text messaging), Hangouts (instant messaging and video chats), Google+ (social networking), Google Groups (group discussions), Google Photos (photo sharing), and YouTube (video sharing); web browsing and search tools such as Google Search (internet searches), Web History (bookmarks and recorded browsing history), and Google Chrome (web browser); online productivity tools such as Google Calendar, Google Contacts, Google Docs (word processing), Google Keep (storing text), Google Drive (cloud storage), Google Maps (maps with driving directions and local business search) and other location services, and Language Tools (text translation); online tracking and advertising tools such as Google Analytics (tracking and reporting on website traffic) and Google AdWords (user targeting based on search queries); Pixel Phone (services which support a Google smartphone); and Google Play (which allow users to purchase and download digital content, e.g., applications).

19. Thus, a subscriber's Google account can be used not only for e-mail but also for other types of electronic communication, including instant messaging and photo and video sharing; voice calls, video chats, SMS text messaging; and social networking. Depending on user settings, user-generated content derived from many of these services is normally stored on Google's servers until deleted by the subscriber. Similar to e-mails, such user-generated content can remain on Google's servers indefinitely if not deleted by the subscriber, and even after being deleted, it may continue to be available on Google's servers for a certain period of time. Furthermore, a Google subscriber can store contacts, calendar data, images, videos, notes, documents, bookmarks, web searches, browsing history, and various other types of information on Google's servers.

20. Based on my training and experience, I know that evidence of who controlled, used, and/or created a Google account may be found within such computer files and other information created or stored by the Google subscriber. Based on my training and experience, I know that the types of data discussed above can include records and communications that constitute evidence of criminal activity.

21. Based on my training and experience, I know that providers such as Google also collect and maintain information about their subscribers, including information about their use of Google services. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. Providers such as Google also commonly have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with other logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which devices were used to access the relevant account. Also, providers such as Google typically collect and maintain location data related to subscriber's use of Google services, including data derived from IP addresses and/or Global Positioning System ("GPS") data.

22. Based on my training and experience, I know that providers such as Google also collect information relating to the devices used to access a subscriber's account – such as laptop or desktop computers, cell phones, and tablet computers. Such devices can be identified in various ways. For example, some identifiers are assigned to a device by the manufacturer and relate to the specific machine or "hardware," some identifiers are assigned by a telephone carrier concerning a particular user account for cellular data or voice services, and some identifiers are actually assigned by Google in order to track what devices are using Google's accounts and services. Examples of these identifiers include unique application number, hardware model, operating system version, Global Unique Identifier ("GUID"), device serial number, mobile network information, telephone number, Media Access Control ("MAC") address, and International Mobile Equipment Identity ("IMEI").

23. Based on my training and experience, I know that such identifiers may constitute evidence of the crimes under investigation because they can be used (a) to find other Google

accounts created or accessed by the same device and likely belonging to the same user, (b) to find other types of accounts linked to the same device and user, and (c) to determine whether a particular device recovered during course of the investigation was used to access the Google account.

24. In addition, I know that Google maintains records that can link different Google accounts to one another, by virtue of common identifiers, such as common e-mail addresses, common telephone numbers, common device identifiers, common 7 computer cookies, and common names or addresses, that can show a single person, or single group of persons, used multiple Google accounts. Based on my training and experience, I also know that evidence concerning the identity of such linked accounts can be useful evidence in identifying the person or persons who have used a particular Google account.

25. Based on my training and experience, I know that subscribers can communicate directly with Google about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Providers such as Google typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

26. In summary, based on my training and experience in this context, I believe that the servers of Google are likely to contain user-generated content such as stored electronic communications (including retrieved and unretrieved e-mail for Google subscribers), as well as Google-generated information about its subscribers and their use of Google services and other online services. In my training and experience, all of that information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. In fact, even if subscribers provide Google with false information about their identities, that false information often nevertheless provides clues to their identities, locations, or illicit activities.

27. As explained above, information stored in connection with a Google account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element of the

offense, or, alternatively, to exclude the innocent from further suspicion. From my training and experience, I know that the information stored in connection with a Google account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, e-mail communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by Google can show how and when the account was accessed or used. For example, providers such as Google typically log the IP addresses from which users access the account along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the Google account access and use relating to the criminal activity under investigation. This geographic and timeline information may tend to either inculpate or exculpate the person who controlled, used, and/or created the account. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent via e-mail). Finally, stored electronic data may provide relevant insight into the user's state of mind as it relates to the offense under investigation. For example, information in the Google account may indicate its user's motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

INVESTIGATION AND PROBABLE CAUSE

28. On or about March 12, 2024 an online tip was received by the FBI National Threat Operations Center (NTOC), regarding the sextortion of an individual in Bangladesh. The report was submitted via email address islam.durjoy@gmail.com, using IP address 2600:c600:3585:97b5:39d2:3511:49b6:18fe, which resolves to Dhaka, Bangladesh.

29. The reporting party, identified as Jane Doe One, advised that she made contact with her local law enforcement in Bangladesh, but that they have no jurisdiction as the threats made to her via email are originating from within the United States.

30. The Bangladesh Police Cyber Crime Unit (BPCCU) was able to utilize a grabify link which your affiant knows to be a tool to assist in the identification or origination of an IP

address. The BPCCU then was able to identify a target IP address of 172.59.33.184, which resolved to Columbus, Ohio.

31. Jane Doe One included in the report made through NTOC some of the messages that she had received from the email account israthshikdar@gmail.com, the **SUBJECT ACCOUNT**. For example, on or about March 5, 2024, Jane Doe One received an email with an attachment that contained three sexually explicit and nude videos depicting Jane Doe One during a previous relationship, prior to her marriage. The body of the message said, "Reply me soon otherwise. I'll send your husband and family members."

32. Jane Doe One stated that she replied to the message from the **SUBJECT ACCOUNT** and then received a series of messages containing additional sexually explicit photos of Jane Doe One and the demand for five million Bangladeshi Taka, which Jane Doe One said equated to approximately $45,000 USD, within 72 hours. Jane Doe One was further advised by the **SUBJECT ACCOUNT** that there were more than one hundred additional images and videos containing Jane Doe One stored on other various external devices. The message read, "I have 100 more video like this. So don't try to do anything wrong. My guys following you and familys every Stap's ##".

33. On or about March 11, 2024, Jane Doe One received another message that read, "If you don't want to give us money then told us don't waste your time and our time. We gonna sell all this videos in dark website. You have 36h"

34. Jane Doe One advised that in July of 2023, she had received phone calls from two unknown numbers: 614-392-9781 and 707-266-7671 and that she knew one of the callers to be Mohammad Rafy, her ex-boyfriend, whom Jane Doe One last knew to live in California. Jane Doe One provided a link to a Facebook page owned by Mohammad Rafy, located at https://www.facebook.com/RaFy.KaNdY?mibextid=ZbWKwL&_rdc=1&rdr , which indicated that he resides in Columbus, Ohio.

35. Using law enforcement databases, Mohammad Rafy was identified and determined to be located in Columbus, Ohio. Specifically, an Ohio Law Enforcement Gateway (OHLEG) search identified Rafy as residing at 5095 Highland Meadows Drive, in Hilliard, Ohio 43026. The OHLEG photo of Rafy appears to match the individual on the Facebook page provided by Jane Doe One. Based on the subject's location, the tip was forwarded to the FBI Cincinnati Office to be followed up on by the Columbus Resident Agency.

36. On or about April 9, 2024, a case was opened to obtain legal process for the identifiers provided by Jane Doe One.

37. On or about May 9, 2024, law enforcement sent an email to Jane Doe One at to request that Jane Doe One forward the original emails and seek further clarification on her original report. For example, law enforcement wanted to determine what Jane Doe One classified as her "early years" and to clarify if Rafy had access to the videos and images being used against her.

38. On or about May 10, 2024, Jane Doe One provided the following bulleted responses of why she believed Rafy was behind the messages:

- Only Rafy had access to those pictures and videos
- Before emailing Jane Doe One in 2024, Rafy contacted Jane Doe One through a WhatsApp number listed as 707-266-7671. That contact occurred in July 2023 during which, Rafy mentioned that Jane Doe one "had to pay for breaking up with [Rafy] in such a way that [Jane Doe One] could never imagine".
- Jane Doe One confirmed Rafy also called her from a different number in June 2023 which was listed as 614-392-9781.

39. Jane Doe One clarified that she had known Rafy from her university days and that the photos and videos that Rafy had were taken when Jane Doe One was between nineteen and twenty-three years of age.

40. Based on the above information, your affiant believes that Rafy is utilizing the **SUBJECT ACCOUNT** which contains images and videos of Jane Doe One and which such content is being used to sextort Jane Doe One for more content.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

41. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(l)(A) and 2703(c)(1)(A), by using the warrant to require Google, LLC to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of **Attachment B**. Upon receipt of the information described in Section I of **Attachment B**, government-authorized persons will review that information to locate the items described in Section II of **Attachment B.**

CONCLUSION

42. Based on the aforementioned factual information, your affiant submits there is probable cause to believe that violations of Title 18, United States Code, Sections 875(d) have been committed, and evidence of those violations is located on the person described in **Attachment A** and in the residence described in **Attachment B**. Your affiant respectfully requests that the Court issue a search warrant authorizing the search and seizure of the items described in **Attachment B**.

43. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. Furthermore, because the warrant will be served on Google, LLC, who will then compile the requested records at a time convenient to it, there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night.

Amanda North Digitally signed by Amanda North DN: CN=Amanda North Reason: I am the author of this document Location: Date: 2024.06.21 12:29:10-04'00' Foxit PDF Editor Version: 13.1.2

Amanda North
TFO
Federal Bureau of Investigation

Sworn to and subscribed before me this 21st day of June, 2024.

Elizabeth A. Preston Deavers
United States Magistrate Judge
United States District Court
Southern District of Ohio

UNITED STATES DISTRICT COURT FOR THE SOUTHERN DISTRICT OF OHIO